CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-007

Sudo Heap-based Buffer Overflow

February 4, 2021 — v1.1

TLP:WHITE

History:

- *02/02/2021 — v1.0 – Initial publication*
- *04/02/2021 — v1.1 – Corrected error in testing command*

Summary

On the 26th of January 2021, Sudo [1] in coordination with Qualys released a security advisory [2, 3] regarding a vulnerability in Sudo allowing any local user on Unix-based system to execute code as root without authentication (privilege escalation).

The vulnerability is exploitable via `sudoedit -s` commands on most systems and several proof-of-concepts were published by security researchers [8].

The potential impact of this vulnerability is high, as an attacker with a low privilege access to any Unix-based system can easily elevate its privileges to completely own the system.

Technical Details

The vulnerability was assigned CVE-2021-3156 [7].

The vulnerability is due to a Heap-Based Buffer Overflow when sudo is executed to run in shell mode through the `-s` or `-i` option.

Normally, sudo escapes special characters when running a command via a shell. However, it is possible to run `sudoedit` with the `-s` or `-i` option in which case no escaping is actually done, making the exploitation of the vulnerability possible.

Qualys security advisory provide a more detailed run-through of the vulnerability [2].

Affected Products

The following versions of sudo are vulnerable:

- All legacy versions from 1.8.2 to 1.8.31p2
- All stable versions from 1.9.0 to 1.9.5p1

All major Linux distribution published security advisories for the vulnerability, as provided on Qualys blog post [3].

Several network devices are based on Unix and are affected by the vulnerability:

- Cisco products [4]
- NetApp products [5]
- F5 products [6]
- ...

Recommendations

Update all servers and devices based on Unix systems to the latest version.

It is possible to test if sudo is vulnerable to CVE-2021-3156 by running one of the following commands (*python*, *perl*, *bash*):

```
sudoedit -s '\' $(perl -e 'print "X" x 65535')
sudoedit -s '\' $(python -c 'print("X"*65535)')
sudoedit -s '\' $(printf "%0.sX" {1..65535})
```

If `sudoedit` crashes with an error, the system is vulnerable to CVE-2021-3156. For example:

- On Arch Linux systems: `malloc(): corrupted top size`
- On Ubuntu systems: `Segmentation fault (core dumped)`

References

[1] https://www.sudo.ws/stable.html#1.9.5p2

[2] https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt

[3] https://blog.qualys.com/vulnerabilities-research/2021/01/26/cve-2021-3156-heap-based-buffer-overflow-in-sudo-baron-samedit

[4] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sudo-privesc-jan2021-qnYQfcM

[5] https://security.netapp.com/advisory/ntap-20210128-0002/

[6] https://support.f5.com/csp/article/K86488846

[7] https://cve.mitre.org/cgi-bin/cvename.cgi?name=2021-3156

[8] https://github.com/lockedbyte/CVE-Exploits/tree/master/CVE-2021-3156

[9] https://github.com/reverse-ex/CVE-2021-3156

[10] https://github.com/blasty/CVE-2021-3156